I. Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 to 23. (Cancelled)

24. (Currently amended) A ~~computerized~~ computer-implemented method for auditing the software or hardware configurations of a plurality of computers in one or more enterprises, comprising the steps of:

in a fully automated manner, collecting from each of a plurality of networked computers configuration information defining each computer's software configuration or hardware configuration or both;

providing a plurality of analyzers based on expert knowledge, each analyzer comprising the executable program steps needed to compute, from selected configuration information gathered from a single computer, a report identifying at least one issue relating to the computer;

defining at least one task definition comprising a list of one or more of said computers and a list of one or more of said analyzers; and

in a fully automated fashion, and guided by one or more of said task definitions --

harnessing each of the task definition's listed analyzers to analyze configuration information gathered from each of the task definition's listed computers;

processing the configuration information so harnessed under the guidance of each analyzer's executable program steps; and

utilizing any issue identifying report generated during the processing step for audit purposes.

25. (Previously presented) A method in accordance with claim 24

wherein the collecting step includes placing this configuration information into a tracker database from which configuration information is later retrieved during the harnessing or processing steps;

wherein the providing analyzers step includes placing these analyzers into an analyzer database from which analyzers are later retrieved during the harnessing or processing steps; and

wherein the processing step includes storing any issue identifying report generated in an issues database from which it may later be retrieved and utilized.

26. (Previously presented) A method in accordance with claim 25 wherein the processing step further includes storing at least some issue identifying reports generated in an issues database together with the identity of the computers whose configuration information was processed to generate those reports and from which issues database both the issue identifying reports and the identity of the computers may later be retrieved and utilized.

27. (Previously presented) A method in accordance with claim 24 wherein the processing step further includes generating, along with at least some issue identifying reports that are generated, the identity of the computers whose configuration information was processed to generate those reports such that both the issue identifying reports and the identity of the computers may be utilized.

28. (Currently amended) A method in accordance with claim 27 which further includes:

providing a plurality of audit report templates;

defining the at least one task definition to further comprise a list of one or more audit report templates; and

following the ~~storing~~ processing step, and guided by the task definition's listed audit report templates and by any issue identifying report generated during the processing step, generating one or more audit reports.

29. (Previously presented) A method in accordance with claim 28

wherein the collecting step includes placing this configuration information into a tracker database from which configuration information may later be retrieved during the harnessing or processing steps;

wherein the providing analyzers step includes placing these analyzers into an analyzer database from which analyzers are later retrieved during the harnessing or processing steps;

wherein the providing audit report templates step includes placing these templates into a report template database from which they may later be retrieved during the audit report generating step; and

wherein the utilizing step includes storing any issue identifying report generated in an issues database from which it may later be retrieved and utilized during the audit report generating step.

30. (Currently amended) A ~~computerized~~ computer-implemented method for auditing the software or hardware configurations of a plurality of computers in one or more enterprises, comprising the steps of:

in a fully automated manner, collecting from each of a plurality of networked computers configuration information defining each computer's software configuration or hardware configuration or both and placing this configuration information into a tracker database;

providing a plurality of analyzers based on expert knowledge, each analyzer comprising the executable program steps needed to compute, from selected configuration information gathered from a single computer, a report identifying at least one issue relating to the computer, and placing these analyzers into an analyzer database;

providing a plurality of audit report templates, and placing these templates into a report template database;

defining at least one task definition comprising a list of one or more of said computers, a list of one or more of said analyzers, and a list of one or more of said audit report templates; and

in a fully automated fashion, and guided by one or more of said task definitions --

harnessing each of the task definition's listed analyzers to analyze configuration information gathered from each of the task definition's listed computers;

processing the configuration information so harnessed under the guidance of each analyzer's executable program steps;

storing any issue identifying reports generated during the processing step in an issues database together with, in at least some instances, the identity of the computers whose configuration information was processed to generate these reports; and

guided by the task definition's listed audit report templates and by any issue identifying reports and computer identities stored in the issues database, generating at least one or more audit reports.

31. (Currently amended) A computerized system for auditing the software or hardware configurations of a plurality of computers in one or more enterprises, the system comprising:

a plurality of computers each computer having software and hardware components configured in a variety of measurable ways;

a network interconnecting said computers;

a plurality of collectors, installed on at least one computer, gathering from said computers configuration information defining each computer's hardware configuration or software configuration or both;

a plurality of analyzers, each analyzer comprising the executable program steps needed to compute, from selected configuration information gathered from a single computer, a report identifying at least one issue relating to the computer;

at least one machine-readable task definition comprising a list of one or more computers and a list of one or more analyzers; and

an analyzer harness guided by said task definition through the process of sequentially harnessing each of the task definition's listed analyzers to analyze configuration information gathered from each of the task definition's listed computers and executing each analyzer's executable program steps upon the harnessed configuration information, thereby generating at least some issue identifying reports.

32. (Previously presented) A system in accordance with claim 31 further comprising:

a tracker database into which said collectors place said gathered configuration information and from which said analyzer harness obtains said configuration information;

an analyzer database in which said analyzers reside and from which said analyzer harness obtains said analyzers; and

an issues database into which said analyzer harness places any generated issue identifying report.

33. (Previously presented) A system in accordance with claim 32

wherein said analyzer harness, in addition to generating issue identifying reports, further generates along with at least some of said reports information identifying the computers whose configuration information was harnessed to generate those issue identifying reports; and

wherein said analyzer harness places both said any generated issue identifying reports and said information identifying computers into said issues database.

34. (Previously presented) A system in accordance with claim 31 wherein said analyzer harness, in addition to generating issue identifying reports, further generates along with at least some of said issue identifying reports information identifying the computers whose configuration information was harnessed to generate those issue identifying reports.

35. (Previously presented) A system in accordance with claim 34 further comprising:

audit report templates;

a list of one or more audit report templates comprising an additional part of said machine-readable task definition; and

a report generator guided by said task definition through the process of transforming at least one of the task definition's listed audit report templates into one or more audit reports, guided by any issue identifying reports and any information identifying computers generated by the analyzer harness.

36. (Previously presented) A system in accordance with claim 35 further comprising:

a tracker database into which said collectors place said gathered configuration information and from which said analyzer harness obtains said configuration information;

an analyzer database in which said analyzers reside and from which said analyzer harness obtains said analyzers;

a report template database containing said audit report templates and from which said report generator obtains said audit report templates; and

an issues database into which said analyzer harness places any generated issue identifying report and any information identifying computers, and from which issues database said report generator obtains issue identifying reports and information identifying computers.

37. (Previously presented) A computerized system for auditing the software or hardware configurations of a plurality of computers in one or more enterprises, the system comprising:

a plurality of computers each computer having software and hardware components configured in a variety of measurable ways;

a network interconnecting said computers with a tracker database;

a plurality of collectors, installed on at least one computer, gathering from said computers configuration information defining each computer's hardware configuration or software configuration or both, and storing the gathered configuration information in the tracker database;

a plurality of analyzers residing within an analyzer database, each analyzer comprising the executable program steps needed to compute, from selected configuration information gathered from a single computer, a report identifying at least one issue relating to the computer;

audit report templates residing within a report templates database;

at least one machine-readable task definition comprising a list of one or more computers, a list of one or more analyzers, and a list of one or more audit report templates;

an analyzer harness connecting to said tracker database and to said analyzer database and guided by said task definition through the process of sequentially harnessing each of the task definition's listed analyzers to analyze configuration information gathered from each of the task definition's listed computers, executing each analyzer's executable program steps upon the harnessed configuration information, and storing any issue identifying reports generated during this execution in an issues database together with, in at least some instances, the identity of the computers whose configuration information was harnessed to generate these issue identifying reports; and

a report generator connecting to said issues database and to said report template database and guided by said task definition through the process of transforming at least one of the task definition's listed audit report templates into one or more audit reports, guided by any issue identifying reports and computer identities stored in the issues database.

38. (Currently amended) A computerized system for auditing the software or hardware configurations of a plurality of computers in one or more enterprises, the system comprising:

a plurality of computers each computer having software and hardware components configured in a variety of measurable ways;

tracker database means, analyzer database means, and issues database means all for storing digital information;

a network interconnecting said computers with said tracker database means;

collector means, installed on at least one computer, for gathering from said computers configuration information defining each computer's hardware configuration or software configuration information or both, and for storing this gathered configuration information in said tracker database means;

analyzer means, residing within said analyzer database means, for defining the executable program steps needed to compute, from selected configuration information gathered from a single computer, a report identifying at least one issue relating to the computer;

machine-readable task definition means for defining a list of one or more computers and a list of one or more analyzer means; and

analyzer harness means connecting to said tracker database means, said analyzer database means, and said issues database means for sequentially harnessing, under the guidance of said task definition means, each of the task definition mean's listed analyzer means to analyze configuration information gathered from each of the task definition mean's listed computers, for executing each analyzer mean's executable program steps upon the harnessed configuration information, and for storing any issue identifying report generated during this execution in said issues database means.

39. (Previously presented) A system in accordance with claim 38

wherein the analyzer harness means, in addition to storing any issue identifying report generated during program step execution in said issues database means, also stores in said issues database means along with at least some issue identifying reports the identities of the computers whose configuration information was harnessed to generate these issue identifying reports.

40. (Previously presented) A system in accordance with claim 38 further comprising:

report template database means for storing digital information;

audit report template means, residing within said report template database means, for defining all or portions of one or more audit reports;

wherein the task definition means further comprises means for defining a list of audit report template means; and

report generator means, connecting to said issues database means and said report template database means, for generating at least one audit report, guided by the task definition mean's listed report templates and by the issue identifying reports stored in the issues database.

41. (Previously presented) A system in accordance with claim 40:

wherein the analyzer harness means, in addition to storing any issue identifying report generated during the program execution step in said issues database means, also stores along with at least some of the issue identifying reports the identities of the computers whose configuration information was harnessed to generate those issue identifying reports; and

wherein the report generator means is also guided by the computer identities stored in the issues database.

42. (Currently amended) A computerized system for auditing the software or hardware configurations of a plurality of computers in one or more enterprises, the system comprising:

a plurality of computers each computer having software and hardware components configured in a variety of measurable ways;

tracker database means, analyzer database means, report template database means, and issues database means all for storing digital information;

a network interconnecting said computers with said tracker database means;

collector means, installed on at least one computer, for gathering from said computers configuration information defining each computer's hardware configuration or software configuration or both, and for storing this gathered configuration information in said tracker database means;

analyzer means, residing within said analyzer database means, for defining the executable program steps needed to compute, from selected configuration information gathered from a single computer, a report identifying at least one issue relating to the computer;

audit report template means, residing within said report template database means, for defining all or portions of one or more audit reports;

machine-readable task definition means for defining a list of one or more computers, a list of one or more analyzer means, and a list of one or more audit report template means;

analyzer harness means connecting to said tracker database means, said analyzer database means, and said issues database means for sequentially harnessing, under the guidance of said task definition means, each of the task definition mean's listed analyzer means to analyze configuration information gathered from each of the task definition mean's listed computers, for executing each analyzer mean's executable program steps upon the harnessed configuration information, and for storing any issue identifying reports generated during this execution [[to]] in said issues database means together with, in at least some instances, the identity of the computers whose configuration information was harnessed to generate these issue identifying reports; and

report generator means, connecting to said issues database means and said report template database means, for generating at least one audit report, guided by the task definition mean's listed report templates and by the issue identifying reports and computer identities stored in the issues database means.